

Lucent Managed Firewall (LMF), Version 4.0 Security Target

Version 1.0

January 17, 2000

Prepared For:

Lucent Technologies
480 Red Hill Road
Room 2B241
Middletown, NJ 07748

Prepared by:



Computer Sciences Corporation
7459A Candlewood Road
Hanover, MD 21076

Table of Contents

1	SECURITY TARGET INTRODUCTION	1
1.1	ST AND TOE IDENTIFICATION	2
1.2	CONVENTIONS, TERMINOLOGY, AND ACRONYMS	3
1.2.1	<i>Conventions</i>	3
1.2.2	<i>Terminology</i>	3
1.2.3	<i>Acronyms</i>	4
1.3	SECURITY TARGET OVERVIEW	5
1.4	COMMON CRITERIA CONFORMANCE CLAIMS.....	6
1.5	EVALUATION TRACEABILITY	6
2	TOE DESCRIPTION OF THE LUCENT MANAGED FIREWALL	7
2.1	APPLICATION CONTEXT.....	7
2.1.1	<i>Evaluation Application Context</i>	7
2.2	PRODUCT TYPE	8
2.3	LMF SCOPE AND BOUNDARIES.....	8
2.3.1	<i>Physical Scope and Boundary</i>	8
2.3.2	<i>Logical Scope and Boundary</i>	9
3	SECURITY ENVIRONMENT	12
3.1	ASSUMPTIONS	12
3.2	THREATS.....	14
3.2.1	<i>Threats To Be Addressed by the LMF</i>	14
3.2.2	<i>Threats To Be Addressed by the Environment</i>	14
3.3	ORGANIZATIONAL SECURITY POLICIES.....	15
4	SECURITY OBJECTIVES.....	16
4.1	SECURITY OBJECTIVES FOR THE TOE.....	16
4.2	SECURITY OBJECTIVES FOR THE ENVIRONMENT	17
5	TOE SECURITY REQUIREMENTS	18
5.1	TOE SECURITY REQUIREMENTS.....	18
5.1.1	<i>TOE Security Functional Requirements</i>	18
5.1.2	<i>TOE Security Assurance Requirements</i>	26
5.1.3	<i>Additional TOE Assurance Requirements</i>	27
5.1.4	<i>Additional Security Assurance Requirements</i>	34
5.2	SECURITY REQUIREMENTS FOR THE IT ENVIRONMENT.....	37
6	TOE SUMMARY SPECIFICATION.....	38
6.1	TOE SECURITY FUNCTIONS	40
6.1.1	<i>Security Management [LMF_SMAN]</i>	40
6.1.2	<i>Identification and Authentication [LMF_INA]</i>	42
6.1.3	<i>User Data Protection [LMF_UDP]</i>	43
6.1.4	<i>Protection of Security Functions [LMF_PSF]</i>	45
6.1.5	<i>Audit [LMF_AUDIT]</i>	46
6.2	ASSURANCE MEASURES.....	49
6.2.1	<i>Configuration Management</i>	50
6.2.2	<i>Delivery and Operation</i>	50
6.2.3	<i>Development</i>	50
6.2.4	<i>Guidance</i>	51

6.2.5	<i>Vulnerability Analysis</i>	51
6.2.6	<i>Test</i>	51
6.2.7	<i>Strength of Function Analysis</i>	52
6.2.8	<i>Maintenance of Assurance</i>	52
7	PP CLAIMS	53
7.1	PP REFERENCE.....	53
7.2	PP REFINEMENTS	53
7.3	PP ADDITIONS	53
7.4	RATIONALE FOR NOT IMPLEMENTING ALL PP SECURITY OBJECTIVES	53
8	RATIONALE	55
8.1	RATIONALE FOR IT SECURITY OBJECTIVES	55
8.2	RATIONALE FOR SECURITY OBJECTIVES FOR THE ENVIRONMENT	56
8.3	RATIONALE FOR SECURITY REQUIREMENTS	58
8.4	RATIONALE FOR ASSURANCE REQUIREMENTS	62
8.5	RATIONALE FOR NOT SATISFYING ALL DEPENDENCIES	63
8.6	CONSISTENCY AND MUTUALLY SUPPORTIVE RATIONALE	63

List of Tables

TABLE 1. LMF ELEMENTS AND THEIR HARDWARE/SOFTWARE COMPONENTS	9
TABLE 2. ASSUMPTIONS FROM THE TFFPP.....	12
TABLE 3. MODIFIED ASSUMPTIONS.....	13
TABLE 4. ADDITIONAL ASSUMPTIONS.....	13
TABLE 5. THREATS	14
TABLE 6. THREATS ADDRESSED BY OPERATING ENVIRONMENT	15
TABLE 7. SECURITY OBJECTIVES	16
TABLE 8. SECURITY OBJECTIVES FOR THE ENVIRONMENT	17
TABLE 9. RESTATED SECURITY FUNCTIONAL REQUIREMENTS	19
TABLE 10. FUNCTIONAL COMPONENTS OMITTED FROM THE TOE	21
TABLE 11. TAILORED TFFPP SFRs	21
TABLE 12. AUDITABLE EVENTS	22
TABLE 13. EAL2 TFFPP SARs.....	26
TABLE 14. TOE ASSURANCE MAINTENANCE REQUIREMENTS.....	27
TABLE 15. ADMINISTRATOR ACCOUNT INFORMATION.....	42
TABLE 16: MAPPING OF THREATS TO SECURITY OBJECTIVES	56
TABLE 17: MAPPINGS BETWEEN THREATS/ASSUMPTIONS AND SECURITY OBJECTIVES FOR THE ENVIRONMENT.....	57
TABLE 18: MAPPINGS BETWEEN TOE SECURITY FUNCTIONS AND IT SECURITY OBJECTIVES	62

Lucent Managed Firewall (LMF) Version 4.0 Security Target

1 SECURITY TARGET INTRODUCTION

- 1 This introductory section presents *security target (ST)* identification information and an overview of the ST structure. A brief discussion of the ST development methodology is also provided.
- 2 An ST document provides the basis for the evaluation of an *information technology (IT)* product or system (e.g., target of evaluation (TOE)). An ST principally defines:
 - A set of assumptions about the security aspects of the environment, a list of threats which the product is intended to counter, and any known rules with which the product must comply (in Section 3, Security Environment).
 - A set of security objectives and a set of security requirements to address that problem (in Sections 4 and 5, Security Objectives and IT Security Requirements, respectively).
- 3 The IT security functions provided by the TOE which meet that set of requirements (in Section 6, TOE Summary Specification).
- 4 The ST for a TOE is a basis for agreement between developers, evaluators, and consumers on the security properties of the TOE and the scope of the evaluation. Because the audience for a ST may include not only evaluators but also developers and "those responsible for managing, marketing, purchasing, installing, configuring, operating, and using the TOE,"¹ this ST minimizes terms of art from the *Common Criteria for Information Technology Security Evaluation (CC)*.
- 5 The structure and contents of this ST comply with the requirements specified in the CC, Part 1, Annex C, and Part 3, Chapter 5.
- 6 A ST, like a Protection Profile (PP), contains sections which address Security Environment, Security Objectives, and IT Security Requirements, as well as Security Objectives Rationale and Security Requirements Rationale sections. Under certain conditions, the contents of these sections of the ST may be identical with those of the PP, namely, when the ST:
 - Claims compliance with the PP.

¹ *Common Criteria for Information Technology Security Evaluation (CC)*, Part 1, C.1, par. 2.

- Performs no additional operations² on the PP security functional requirements.
- Does not extend the PP by adding security objectives and/or security requirements.

7 Under these conditions, the CC states that "*reference* to the PP is sufficient to define and justify the TOE objectives and requirements. *Restatement of the PP contents is unnecessary*" [italics added].³

8 The methodology used to develop and present this ST includes the following steps:

- Those PP security objectives and requirements with which the ST claims compliance and for which no additional operations are to be performed are restated within the ST verbatim.
- If the ST will perform additional operations on PP requirements, the ST restates the requirements, performs the operations, and identifies the change by convention.
- If the ST extends the PP by adding security objectives and/or security requirements, the ST states the objectives and/or requirements, makes any needed additions to the Security Environment section, and documents suitable Rationale sections.

1.1 ST and TOE Identification

9 This section provides information needed to identify and control this ST and its TOE, the Lucent Managed Firewall (LMF) Version 4.0. This ST targets an Evaluation Assurance Level (EAL) 2 level of assurance.

ST Title: Lucent Managed Firewall (LMF) Version 4.0
Security Target, Version 1.0, January 17, 2000.

TOE Identification: Lucent Managed Firewall (LMF) Version 4.0

CC Identification: Common Criteria for Information Technology
Security Evaluation, Version 15408, FDIS,
ISO/IEC SC27 N2162, 15 November 1998

PP Identification: U.S. Government Traffic-Filter Firewall
Protection Profile for Low-Risk Environments,
Final, Version 1.1 April 1999 (referred to as
TFFPP)

² The CC allows controlled tailoring of its security functional requirements, by means of four *operations* (namely, refinement, selection, assignment, and iteration; see CC, Part 2, par. 2.1.4).

³ CC, Part 1, Annex C, par. C.2.8, b.

ST Evaluation: Computer Science Corporation (CSC)

Keywords: information flow control, firewall, packet filter, network security, traffic filter, security target

1.2 Conventions, Terminology, and Acronyms

10 This section identifies the formatting conventions used to convey additional information and terminology having specific meaning. It also defines the meanings of abbreviations and acronyms used throughout the remainder of the document.

1.2.1 Conventions

11 This section describes the conventions used to denote CC operations on security requirements and to distinguish text with special meaning. The notation, formatting, and conventions used in this ST are largely consistent with those used in the CC. Selected presentation choices are discussed here to aid the Security Target reader.

12 The CC allows several operations to be performed on functional requirements; *assignment*, *iteration*, *refinement*, and *selection* are defined in paragraph 2.1.4 of Part 2 of the CC.

- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment is indicated by showing the value in square brackets [assignment_value(s)].
- The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**.
- The selection operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *underlined italicized text*.
- Plain *italicized text* is used for both official document titles and text meant to be emphasized more than plain text.

1.2.2 Terminology

13 In the Common Criteria, many terms are defined in Section 2.3 of Part 1. The following terms are a subset of those definitions. They are listed here to aid the user of the Security Target.

<i>User</i>	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
<i>Human user</i>	Any person who interacts with the TOE.
<i>External IT entity</i>	Any IT product or system, untrusted or trusted,

outside of the TOE that interacts with the TOE.

Role

A predefined set of rules establishing the allowed interactions between a user and the TOE.

Identity

A representation (e.g., a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.

Authentication data

Information used to verify the claimed identity of a user.

- 14 In addition to the above general definitions, this Security Target provides the following specialized definitions:

Authorized Administrator – A role which human users may be associated with to administer the security parameters of the TOE. Such users are not subject to any access control requirements once authenticated to the TOE and are therefore trusted to not compromise the security policy enforced by the TOE.

Authorized external IT entity – Any IT product or system, outside the scope of the TOE that may administer the security parameters of the TOE. Such entities are not subject to any access control requirements once authenticated to the TOE and are therefore trusted to not compromise the security policy enforced by the TOE.

1.2.3 Acronyms

- 15 The following abbreviations from the Common Criteria are used in this Security Target:

CC	Common Criteria for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
IT	Information Technology
PP	Protection Profile
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

1.3 Security Target Overview

- 16 The LMF architecture consists of two physically distinct components:
- ◆ The Firewall Appliance (FA), which controls the flow of Internet Protocol (IP) traffic (datagrams) between network interfaces; and
 - ◆ The Security Management Server (SMS) software, by means of which administrators manage the security of one or more Firewall Appliances.
- 17 The firewall code runs on Inferno™, a small Bell Labs-developed operating system. The separate Security Management Server software, implemented as Inferno daemons and Java applets, runs on Hosted Inferno and Netscape Enterprise Server, v4.0, respectively; the latter runs either on Windows NT™ or Sun Solaris™⁴ operating systems.
- 18 The FA controls the flow of IP datagrams based on security policy rules. As with other traffic filter firewalls, the FA controls the flow of datagrams based upon the interface of arrival, interface of egress, source and destination addresses, higher protocol and ports, and action to be taken (pass or drop).
- 19 Policy rules are defined by authorized administrators using the SMS. The SMS also supports the management of the other LMF security features, notably, of audit (for example, event selection, reports, and routing of selected audit event information to console, email, syslog, or beeper) and of administrator accounts.
- 20 The administrative interface to the SMS is via a Netscape Communicator browser; it is implemented by Java applets. In the evaluated configuration, the browser runs on the same platform as the SMS.
- 21 All communications between a FA and the SMS are encrypted and authenticated using native Inferno™ encryption and authentication mechanisms (Diffie Hellman for key exchange, ElGamal for digital signatures and signature verification, Triple DES for session encryption).
- 22 The secure configuration for evaluation is the basic network configuration as described in Lucent Managed Firewall Version 4.0, Delivery, Installation, Generation, and Start-Up Procedures.. The protected network is connected to one interface, the isolated SMS network to a second, and the external network (via a router) to a third.

⁴ The evaluation configuration uses Windows NT™ platform.

1.4 Common Criteria Conformance Claims

- 23 The TOE conforms to the U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments, Version 1.1, FINAL. It also conforms to Parts 2 and 3 of the CC, Version 15408 FDIS, ISO/IEC SC27 N2161.

1.5 Evaluation Traceability

- 24 The LMF v3.0 has been successfully evaluated against the Security Target, v1.1, for the Lucent Managed Firewall (LMF), v3.0, December 8, 1998 at the EAL2 level of assurance.

2 TOE DESCRIPTION OF THE LUCENT MANAGED FIREWALL

25 This section provides context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

2.1 Application Context

26 The LMF can be used either by an enterprise, where the firewall is located on enterprise premises, or by an Internet Service Provider (ISP), where the firewall is located in the ISP's network. Whether employed by enterprise or ISP, the LMF is useful in a variety of configurations. For example:⁵

- a) A FA can be placed at the perimeter of an enterprise's intranet to protect it from the Internet.
- b) Building upon the previous configuration, one can add a "demilitarized zone" (DMZ), in which to place the enterprise's publicly available Web servers, for example.
- c) Multiple FA's can be placed to control several security zones within the enterprise intranet.
- d) An ISP can manage multiple FA's with a single SMS, and, using the LMF security zone feature, can allow different customers to control their own security policies.

27 For details regarding these and other configurations outside the scope of the evaluation, see the LMF *Functional Specification and High-Level Design Document*, "Application Scenarios."

2.1.1 Evaluation Application Context

28 The following physical and logical boundaries are drawn around the above mentioned configurations to scope the TOE evaluation. For the TOE to be conformant with the TFFPP and satisfy this ST, the TOE configuration must conform to the following specifications:

29 The secure configuration of the LMF must be configured in accordance with (IAW) the directives contained in the Installation, generation and start-up (IGS) documentation.

30 The configured SMS must be physically isolated from user networks.

31 The configured LMF must be physically protected as a single co-located entity.

⁵ This is provided merely as an example. The evaluated LMF configuration consists of one SMS and one FA. At minimum, the LMF physical boundary includes just these two components. The secure configuration for evaluation is the basic network configuration as described in *Lucent Managed Firewall Version 4.0, Delivery, Installation, Generation, and Start-Up Procedures*. The protected network is connected to one interface, the isolated SMS network to a second, and the external network (via a router) to a third.

- 32 The LMF must be configured to have only an SMS and one FA.
- 33 The configured SMS must be isolated from communication (e.g., through rules enforced by the FA) with any other connected network.
- 34 In the configured LMF, the SMS must be used only for the administration of FA's. (The SMS must not use the Netscape Server to host web pages or provide word processing applications, etc.)

2.2 Product Type

- 35 This section identifies the LMF's product type.
- 36 The LMF is a traffic-filter firewall. A traffic-filter firewall controls the flow of individual Internet Protocol (IP) datagrams by matching information contained in IP and higher layer headers against a set of rules specified by the firewall's administrator. This header information includes source and destination host IP addresses, source and destination port numbers, and upper level protocol identifier (for transmission control protocol (TCP) or user datagram protocol (UDP), e.g.). Depending upon the rule and the results of the match, the firewall either passes or drops the packet. In addition to protocol header information, traffic-filter firewalls use other information, such as the direction (incoming or outgoing) of the packet on a given firewall interface.

2.3 LMF Scope and Boundaries

- 37 This section provides a general description of the physical and logical scope and boundaries of the LMF.

2.3.1 Physical Scope and Boundary

- 38 As stated in Section 1.3 above, the Lucent Managed Firewall architecture consists of two physically distinct components:
- ◆ The FA, which controls the flow of IP datagrams between network interfaces; and
 - ◆ The SMS software, by means of which administrators manage the security of multiple FA's.
- 39 The evaluated LMF configuration consists of one SMS and one FA. At minimum, the LMF physical boundary includes just these two components. The secure configuration for evaluation is the basic network configuration as described in the *Lucent Managed Firewall Version 4.0, Delivery, Installation, Generation, and Start-Up Procedures*. The protected network is connected to one interface, the isolated SMS network to a second, and the external network (via a router) to a third.

40 The physical scope of the LMF includes the hardware and software components identified in Table 1.

Table 1. LMF Elements and Their Hardware/Software Components

LMF Element	Hardware/Software Components
Firewall Appliance	Intel x86 processor; 4MB flash disk; four 10/100BaseT Ethernet interface cards; RS-232 port for failover; floppy disk drive
	Inferno™ operating system
Security Management Server	400 MHz Pentium processor (minimum); 256 MB system memory; 4 GB hard disk; CD-ROM drive; Ethernet interface card; Video card capable of 1024 x 768 resolution with 65,535 colors; backup device (e.g., tape, zip drive, or Syquest drive)
	Microsoft Windows NT Workstation 4.0 with Service Pack 4; Netscape Enterprise Server 3.5.1; Netscape Communicator 4.05 Adobe Acrobat Reader 3.01

41 The LMF has eleven major subsystems. For an account of them, see the LMF *Functional Specification and High-Level Design Document*.

2.3.2 Logical Scope and Boundary

42 The security functional requirements implemented by the LMF are usefully grouped under the following classes or families:

43 *Access Control*:⁶ the FA controls the flow of incoming and outgoing IP datagrams.

44 *Audit*: the FA detects the occurrence of selected events, gathers information concerning them, and sends that information to the SMS, where it is stored. The SMS also detects the occurrence of selected events (e.g., security administrator actions), gathers information concerning them, and records it. Audit reporting features are also provided by the SMS. Included among the reporting features is the routing of selected audit

⁶ Books on firewalls typically identify "access control" as a firewall's central security mechanism. The *Common Criteria* (CC) distinguishes "access control" from "information flow control"; and the TFF PP specifies (not access control but) information flow control requirements for firewalls. Here, the term "access control" is used in the broader sense known to the firewall community, in order to facilitate the understanding of firewall developers, marketers, and others unfamiliar with the *Common Criteria*'s terms of art.

event information to console, email, syslog, or beeper, as selected by an authorized administrator.

45 *Identification and Authentication (I&A):* the FA has no user (including administrator) accounts. The SMS requires administrators to identify and authenticate themselves before they can perform any other SMS actions.

46 *Security Management:* the SMS provides all LMF security management capabilities. By means of it, administrators manage the security policy rules enforced by associated FA's, audit mechanism configuration parameters, and administrator accounts.

47 *Protection of Security Functions:* the FA security functions which implement the LMF access control policy,⁷ are physically separated from the unauthenticated external IT entities which send and receive IP datagrams through the FA; and the design of these functions is such that they cannot be bypassed by those external IT entities.

48 The LMF logical boundary includes the FA's and the SMS. The evaluated secure configuration must contain the same physical and logical isolation. The logical scope of the LMF extends to the five classes or families of security functional requirements just mentioned.

49 The LMF also provides the following capabilities, but they fall outside the scope of this evaluation:

50 Remapping source and destination host addresses to other internal addresses, using Network Address Translation (NAT);

51 Protecting the confidentiality and integrity of an enterprise's messages by means of Virtual Private Networks (VPNs) between the enterprise's FA's, using IP Security Protocol (IPSEC) encryption and cryptographic checksums; and

52 Dividing administrative responsibilities between a LMF system administrator role and one or more LMF zone administrators, each of which manages the security of a subset of the FA's associated with an SMS. The TFF PP requires a single "authorized administrator" role, and the LMF System Administrator role meets this requirement.⁸

53 These additional capabilities are not required by the TFFPP and are not part of this evaluation of the LMF.

54 Remote administration of the LMF is another capability that falls outside the scope of this evaluation. The LMF does not itself provide the

⁷ More precisely, they implement the information flow control policy named "UNAUTHENTICATED SFP" (Security Function Policy) by the TFF PP.

⁸ Although the zone administrator role is not part of the evaluated LMF configuration, security zones are.

capability for authorized administrators to remotely administer the SMS. Remote administration of the SMS can be achieved by the following (out of evaluation scope) method: *Administrators obtain a digital ID from Verisign. The digital ID is used to establish Secure Sockets Layer (SSL) sessions between the Netscape Enterprise Server and the Netscape Communicator browser on the remote platform.*

3 SECURITY ENVIRONMENT

55 This section aims to clarify the nature of the security problem that the LMF is intended to solve. It does so by describing:

56 Any *assumptions* about the security aspects of the environment and/or of the manner in which the LMF is intended to be used

57 Any known or assumed *threats* to the assets against which specific protection within the LMF or its environment is required

58 Any *organizational security (OSP)* statements or rules with which the LMF must comply

59 The LMF, v4.0 is intended to be used either in environments in which, at most, sensitive but unclassified information is processed, or the sensitivity level of information in both the internal and external networks is equivalent.

3.1 Assumptions

60 This section helps define the scope of the security problem by identifying assumptions about the security aspects of the environment and/or of the manner in which the LMF is intended to be used.

61 The TOE claims all the assumptions delineated within Section 3.1 of the TFFPP. Those assumptions that are claimed are stated verbatim in Table 2 below:

Table 2. Assumptions from the TFFPP

Name	Description
A.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
A.PUBLIC	The TOE does not host public data.
A.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
A.SINGEN	Information can not flow among the internal and external networks unless it passes through the TOE

62 Four additional security environment assumptions described in the TFFPP have been modified in this ST. Table 3 states these modified assumptions. The refined assumptions are applicable to the architecture of this specific TOE.

Table 3. Modified Assumptions

Name	Description
A.GENPUR	The TOE only stores and executes security-relevant applications and only stores data required for its secure operation.
A.DIRECT	The TOE is available to authorized administrators only.
A.NOREMO	With the exception of identification and authentication, human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.
A.PHYSEC	The processing resources of the TOE that depend on hardware security features will be located within controlled access facilities that mitigate unauthorized, physical access.

63 An additional security assumption for the environment not described in the TFFPP has been included in this ST. Table 4 states this additional assumption.

Table 4. Additional Assumptions

Name	Description
A.SECFUN	With the exception of identification and authentication, there are no security functions on the TOE accessible to human users who are not authorized administrators.

64 In addition to the above assumptions, the following assumptions about the TOE and the TOE environment are also made:

- a) The secure configuration for evaluation will be the basic network configuration as described in Section 3 of the *Lucent Managed Firewall Version 4.0, Delivery, Installation, Generation, and Start-Up Procedures* (Version 8.1)
- b) The protected network is connected to one interface, the isolated SMS network to a second, and the external network (via a router) to a third.
- c) The evaluated secure configuration must contain the same physical and logical isolation.
- d) Because of the physical and logical isolation, the A.REMACC secure usage assumption is not included. Remote administration will not be part of evaluated secure configuration functionality.

3.2 Threats

65 This section helps define the nature and scope of the security problem by identifying assets which require protection as well as threats to those assets.

66 Threats may be addressed either by the LMF or by its intended environment (for example, using personnel, physical, or administrative safeguards). These two classes of threats are discussed separately.

3.2.1 Threats To Be Addressed by the LMF

67 The TOE addresses all threats delineated within Section 3.2.1 of the TFFPP. For clarity, these threats are restated verbatim in Table 5.

Table 5. Threats

Name	Description
T.NOAUTH	An unauthorized user may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.
T.ASPOOF	An unauthorized person may carry out spoofing in which information flow through the TOE into a connected network by using a spoofed source address.
T.MEDIAT	An unauthorized person may send impermissible information through the TOE that results in the exploitation of resources on the internal network.
T.OLDINF	Because of a flaw in the TOE functioning, an unauthorized person may gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows from the TOE.
T.AUDACC	Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.
T.SELPRO	An unauthorized user may read, modify, or destroy security critical TOE configuration data.
T.AUDFUL	An unauthorized person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attackers actions.

3.2.2 Threats To Be Addressed by the Environment

68 The TOE Operating Environment addresses the same TFFPP, Section 3.2.2 Threat To Be Addressed by Operating Environment. This threat has

been adapted for the LMF because the physical and logical isolation dictated by the evaluated secure configuration, and the precluding of remote administration, results in only trusted (administrators) accessing the LMF. The adapted version is provided in the following Table 6. Also, a threat to the TOE is repeated as a threat to the operating environment.

Table 6. Threats Addressed by Operating Environment

Name	Description
T.TUSAGE	The TOE may be used and administered in an insecure manner.
T.AUDACC	Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.

3.3 Organizational Security Policies

69 This section identifies and explains any OSPs with which the LMF must comply in addressing the security problem.

70 The TFFPP states one OSP relating to the use of cryptographic modules. Because this TOE is not providing remote administration, this OSP does not apply. Therefore, no organizational security policy is specified.

4 SECURITY OBJECTIVES

71 The purpose of the security objectives is to detail the planned response to a security problem or threat. Threats can be directed against the TOE or the security environment or both, therefore, the CC identifies two categories of security objectives:

(1) Security objectives for the TOE, and

(2) Security objectives for the Operating Environment.

4.1 SECURITY OBJECTIVES FOR THE TOE

72 The TOE accomplishes a subset of the security objectives delineated within Section 4.1 of the TFFPP. For clarity, these security objectives are restated in Table 7.

Table 7. Security Objectives

Name	Description
O.IDAUTH	The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions or, for certain specified services, to a connected network.
O.MEDIAT	The TOE must mediate the flow of all information between users on an internal network connected to the TOE and users on an external network connected to the TOE, and must ensure that residual information from a previous information flow is not transmitted in any way.
O.SECSTA	Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.
O.SELPRO	The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.
O.AUDREC	The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes.
O.ACCOUN	The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions.

Name	Description
O.SECFUN	The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.

4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT

73 Eleven security objectives for the TOE environment are those specified in the following Table 8 and are derived from the assumptions stated in the TFFPP, Section 4.2.

Table 8. Security Objectives for the Environment

Name	Description
O.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
O.PUBLIC	The TOE does not host public data.
O.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
O.SINGEN	Information can not flow among the internal and external networks unless it passes through the TOE
O.SECFUN	With the exception of identification and authentication, there are no security functions on the TOE accessible to human users who are not authorized administrators.
O.NOREMO	With the exception of identification and authentication, human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.
O.GUIDAN	Those responsible for the TOE must ensure that the TOE is delivered, installed, administered, and operated in a manner that maintains security.
O.ADMTRA	Authorized administrators are trained as to establishment and maintenance of sound security policies and practices.
O.PHYSEC	The processing resources of the TOE that depend on hardware security features will be located within controlled access facilities that mitigate unauthorized, physical access.
O.GENPUR	The TOE only stores and executes security-relevant applications and only stores data required for its secure operation.
O.DIRECT	The TOE and associated direct-attached console are available to authorized administrators only.

5 TOE SECURITY REQUIREMENTS

74 IT security requirements include:

- a) TOE security requirements and (optionally)
- b) Security requirements for the TOE's IT environment (that is, for hardware, software, or firmware external to the TOE and upon which satisfaction of the TOE's security objectives depends).

75 These requirements are discussed separately below.

5.1 TOE Security Requirements

76 The CC divides security requirements into two categories:

- a) *Security functional requirements (SFRs)*, that is, requirements for security functions such as information flow control, audit, identification and authentication.
- b) *Security assurance requirements (SARs)*, provide grounds for confidence that the TOE meets its security objectives (for example, configuration management, testing, vulnerability assessment).

77 This section presents the security functional and assurance requirements for the TOE.

5.1.1 TOE Security Functional Requirements

78 This section presents the SFRs for the TOE. In accordance with the methodology described in Section 1.4, Security Target Preparation Methodology, this section has the following five subsections:

- a) *Restated PP SFRs*: those PP security functional requirements with which the ST claims compliance⁹ and for which no additional operations are to be performed. These PP SFRs are included in the ST verbatim.
- b) *Omitted PP SFRs* those PP security functional requirements that have been omitted from this ST because the evaluated configuration of LMF Version 4.0 does not support Remote Administration of the TOE.
- c) *Tailored PP SFRs*: those PP security functional requirements with which the ST claims compliance but for which additional operations are to be performed.
- d) *Additions to PP SFRs* (optional): any security functional requirements additional to those of the PP.

⁹ Compliance is based on incorporation of the changes recommended in ORs against the TFFPP.

- e) *SFRs With Strength of Function (SOF) Declarations*: any security functional requirement that requires a SOF declaration.

5.1.1.1 Restated PP SFRs

79 The TOE shall satisfy the SFRs stated in Table 9 which lists the CC names of the SFR components¹⁰ contained in the TFFPP. Following the table, the individual functional requirements are restated from the TFFPP.

Table 9. Restated Security Functional Requirements

Functional Component ID	Functional Component Name
FAU_SAR.1	Audit review
FAU_STG.4	Prevention of audit data loss
FDP_IFC.1	Subset information flow control
FDP_RIP.1	Subset residual information protection
FIA_UAU.1	Timing of authentication
FIA_UID.2	User identification before any action
FMT_SMR.1	Security roles
FPT_RVM.1	Non-bypassability of the TSP
FPT_SEP.1	TSF domain separation
FPT_STM.1	Reliable time stamps

- 80 FAU_SAR.1 Audit review
- FAU_SAR.1.1 The TSF shall provide [an authorized administrator] with the capability to read [all audit trail data] from the audit records.
- FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.
- 81 FAU_STG.4 Prevention of audit data loss
- FAU_STG.4.1 The TSF shall prevent auditable events except those taken by the **authorized administrator** and [shall limit the number of audit records lost] if the audit trail is full.
- 82 FDP_IFC.1 Subset information flow control
- FDP_IFC.1.1 The TSF shall enforce the [UNAUTHENTICATED SFP] on:
- a) [subjects: unauthenticated external IT entities that send and receive information through the TOE to one another.
 - b) information: traffic sent through the TOE from one subject to another;
 - c) operation: pass information.]

¹⁰ In CC parlance, a *component* is "the smallest set of selectable [requirements] elements that may be included in a PP" or an ST (CC, Part 1, 2.3). An element is "An indivisible security requirement" (*ibid.*).

- 83 FDP_RIP.1 Subset residual information protection
- FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the allocation of the resource to the following objects: [resources that are used by the subjects of the TOE to communicate through the TOE to other subjects].
- 84 FIA_UAU.1 Timing of authentication
- FIA_UAU.1.1 The TSF shall allow [identification as stated in FIA_UID.2] on behalf of the authorized administrator or authorized external IT entity accessing the TOE to be performed before the authorized administrator or authorized external IT entity is authenticated.
- FIA_UAU.1.2 The TSF shall require each authorized administrator or authorized external IT entity to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that authorized administrator or authorized IT entity.
- 85 FIA_UID.2 User identification before any action
- FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.
- 86 FMT_SMR.1 Security roles
- FMT_SMR.1.1 The TSF shall maintain the role [authorized administrator].
- FMT_SMR.1.2 The TSF shall be able to associate **human** users with **the authorized administrator** role.
- 87 FPT_RVM.1 Non-bypassability of the TSP
- FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.
- 88 FPT_SEP.1 TSF domain separation
- FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.
- FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.
- 89 FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

5.1.1.2 Omitted PP SFRs

90 The TFFPP specifies that some functional requirements are optional and may be omitted from compliant TOEs. Table 10 identifies the SFRs that have been omitted from this ST because the evaluated configuration of LMF Version 4.0 does not support Remote Administration of the TOE.

Table 10. Functional Components Omitted from the TOE

Reference	Description
FCS_COP.1	Cryptographic operation
FIA_AFL.1	Authentication failure handling
FIA_UAU.4	Single-use authentication mechanisms

5.1.1.3 Tailored PP SFRs

91 The TFFPP identifies several SFRs that contain operations to be completed in PP-compliant security targets. This section identifies those TFFPP requirements and performs the required operations. The TOE shall satisfy the resultant requirements.

92 Table 11 names the SFRs for which the ST is required to perform operations. The table also identifies the operations (assignment, iteration, refinement, and selection) performed on them in this ST. Following the table, the individual functional requirements are restated from the TFFPP, and the operations completed.

Table 11. Tailored TFFPP SFRs

Functional Component ID	Functional Component Name	Operation
FAU_GEN.1	Audit data generation	Refinement Selection
FAU_SAR.3	Selectable audit review (1)	Iteration
FAU_SAR.3	Selectable audit review (2)	Assignment Iteration
FAU_STG.1	Protected audit trail storage	Refinement
FDP_IFF.1	Simple security attributes	Assignment Refinement
FIA_ATD.1	User attribute definition	Assignment
FMT_MSA.3	Static attribute initialization	Assignment Refinement Selection
FMT_MOF.1	Management of security functions behavior	Refinement

93 FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

- a) Start-up and shutdown of the audit functions;
- b) All **relevant** auditable events for the *minimal or basic* level of audit **specified in Table 12**; and
- c) [the event in **Table 12** listed at the “extended” level.]

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

- a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
- b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [information specified in column four of **Table 12**.]

Table 12. Auditable Events

Functional Component	Level	Auditable Event	Additional Audit Record Contents
FMT_SMR.1	minimal	Modifications to the group of users that are part of the authorized administrator role.	The identity of the authorized administrator performing the modification and the user identity being associated with the authorized administrator role
FIA_UID.2	basic	All use of the user identification mechanism.	The user identities provided to the TOE
FIA_UAU.1	basic	Any use of the authentication mechanism.	The user identities provided to the TOE
FDP_IFF.1	basic	All decisions on requests for information flow.	The presumed addresses of the source and destination subject.
FCS_COP.1	minimal	Success and failure, and the type of cryptographic operation	The identity of the external IT entity attempting to perform the cryptographic operation
FPT_STM.1	minimal	Changes to the time.	The identity of the authorized administrator performing the operation
FMT_MOF.1	extended	Use of the functions listed in this requirement pertaining to audit.	The identity of the authorized administrator performing the operation

94

FAU_SAR.3 Selectable audit review (1)

FAU_SAR.3.1 The TSF shall provide the ability to perform searches of audit data based on

- a) [user identity;
- b) presumed subject address;

- c) ranges of dates;
- d) ranges of times;
- e) ranges of addresses.]

95 FAU_SAR.3 Selectable audit review (2)

FAU_SAR.3.1 The TSF shall provide the ability to perform sorting of audit data based on

- a) [the chronological order of audit event occurrence.]

96 FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to prevent modifications to the audit records **by users other than an authorized administrator.**

97 FDP_IFF.1 Simple security attributes¹¹

FDP_IFF.1.1 The TSF shall enforce the [UNAUTHENTICATED SFP] based on the following types of subject and information security attributes:

- a) [SUBJECT attributes:
 - 1) presumed address;
 - 2) {no other subject attributes}.
- b) INFORMATION attributes:
 - 1) presumed address of source subject;
 - 2) presumed address of destination subject;

¹¹. The complete set of functional elements of a component must be selected for inclusion in a PP. However, since the following functional elements from the FDP_IFF.1 component do not add anything significant to the PP, they have been moved here to allow for a clearer, smoother flowing presentation of FDP_IFF.1.

FDP_IFF.1.3 - The TSF shall enforce the [none].

FDP_IFF.1.4 - The TSF shall provide the following [none].

FDP_IFF.1.5 - The TSF shall explicitly authorize an information flow based on the following rules: [none].

- 3) transport layer protocol;
- 4) TOE interface on which traffic arrives and departs;
- 5) service;
- 6) {no other information security attributes}].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and **another** controlled **subject** via a controlled operation if the following rules hold:

- a) [Subjects on an internal network can cause information to flow through the TOE to another connected network if:
 - 1) all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;
 - 2) the presumed address of the source subject, in the information translates to an internal network address;
 - 3) and the presumed address of the destination subject, in the information, translates to an address on the other connected network.
- b) Subjects on the external network can cause information to flow through the TOE to another connected network if:
 - 1) all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;
 - 2) the presumed address of the source subject, in the information translates to an external network address;
 - 3) and the presumed address of the destination subject, in the information, translates to an address on the other connected network.]

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules:

- a) [The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed address of the source subject is an external IT entity on an internal network;
- b) The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the presumed address of the source subject is an external IT entity on the external network;
- c) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on a broadcast network;

- d) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on the loopback network;
- e) **The TOE shall reject requests in which the subject specifies the route in which information shall flow en route to the receiving subject;**

98

FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

- a) [Identity
- b) association of a human user with the authorized administrator role;
- c) {no other user security attributes.}]

99

FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the [information flow control **UNAUTHENTICATED** SFP] to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow an [authorized administrator] to specify alternative initial values to override the default values when an object or information is created.

100

FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to perform the functions

- a) [start-up and shutdown;
- b) create, delete, modify, and view information flow security policy rules that permit or deny information flows;
- c) create, delete, modify, and view user attribute values defined in FIA_ATD.1;
- d) enable and disable single-user authentication mechanisms in FIA_UAU.4;
- e) modify and set the threshold for the number of permitted authentication attempt failures;
- f) restore authentication capabilities for users that have met or exceeded the threshold for permitted authentication attempt failures;
- g) enable and disable external IT entities from communicating with the TOE ;
- h) modify and set the time and date;
- i) archive, create, delete, empty, and review the audit trail;

- j) backup of user attribute values, information flow security policy rules, and audit trail data, where the backup capability shall be supported by automated tools;
 - k) recover to the state following the last backup
 - l) additionally, if the TSF supports remote administration from either an internal or external network:
 - 1) enable and disable remote administration from internal and external networks;
 - 2) restrict addresses from which remote administration can be performed;
 - m) {no other services}}
- to an authorized administrator.

5.1.1.4 Additions to PP SFRs

- 101 The ST has no additional requirements beyond those already stated in the TFFPP.

5.1.1.5 SFRs With SOF Declarations

- 102 FIA_UAU.1 The FIA_UAU.1 SFR requires that the TOE have an authentication mechanism that has a probability of authentication data being guessed will be less than one in a million.

- 103 The overall Strength of function claim for the TOE is SOF-basic.

5.1.2 TOE Security Assurance Requirements

- 104 Table 13 identifies the security assurance components drawn from CC Part 3: Security Assurance Requirements, EAL2. The assurance requirements are stated verbatim from TFFPP section 5.1.2, TOE Security Assurance Requirements.

Table 13. EAL2 TFFPP SARs

Assurance Component ID	Assurance Component Name
ACM_CAP.2	Configuration Items
ADO_DEL.1	Delivery procedures
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.1	Informal functional specification
ADV_HLD.1	Descriptive high-level design
ADV_RCR.1	Informal correspondence demonstration
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ATE_COV.1	Evidence of coverage
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_SOF.1	Strength of TOE security function evaluation
AVA_VLA.1	Developer vulnerability analysis

5.1.3 Additional TOE Assurance Requirements

105 In addition to the EAL 2 assurance requirements stated in the PP, the assurance maintenance requirements in Table 14 are included for the TOE.

Table 14. TOE Assurance Maintenance Requirements

Assurance Component ID	Assurance Component Name
ALC_FLR.1	Basic flaw remediation
AMA_AMP.1	Assurance maintenance plan
AMA_CAT.1	TOE component categorization report

5.1.3.1 ACM_CAP.2 Configuration items

106 Developer action elements :

ACM_CAP.2.1D The developer shall provide a reference for the TOE.

ACM_CAP.2.2D The developer shall use a CM system.

ACM_CAP.2.3D The developer shall provide CM documentation.

107 Content and presentation of evidence elements :

ACM_CAP.2.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.2.2C The TOE shall be labelled with its reference.

ACM_CAP.2.3C The CM documentation shall include a configuration list.

ACM_CAP.2.4C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.2.5C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.2.6C The CM system shall uniquely identify all configuration items.

108 Evaluator action elements :

ACM_CAP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.1.3.2 ADO_DEL.1 Delivery procedures

109 Developer action elements :

ADO_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.1.2D The developer shall use the delivery procedures.

110 Content and presentation of evidence elements :

ADO_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

111 Evaluator action elements :

ADO_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.1.3.3 ADO_IGS.1 Installation, generation, and start-up procedures

112 Developer action elements :

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

113 Content and presentation of evidence elements :

ADO_IGS.1.1C The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

114 Evaluator action elements :

ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2E The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.1.3.4 ADV_FSP.1 Informal functional specification

115 Developer action elements :

ADV_FSP.1.1D The developer shall provide a functional specification.

116 Content and presentation of evidence elements :

ADV_FSP.1.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2C The functional specification shall be internally consistent.

ADV_FSP.1.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

ADV_FSP.1.4C The functional specification shall completely represent the TSF.

117 Evaluator action elements :

ADV_FSP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.1.3.5 ADV_HLD.1 Descriptive high-level design

118 Developer action elements :

ADV_HLD.1.1D The developer shall provide the high-level design of the TSF.

119 Content and presentation of evidence elements :

ADV_HLD.1.1C The presentation of the high-level design shall be informal.

ADV_HLD.1.2C The high-level design shall be internally consistent.

ADV_HLD.1.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.1.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.1.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.1.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.1.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

120 Evaluator action elements :

ADV_HLD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.1.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.1.3.6 ADV_RCR.1 Informal correspondence demonstration

121 Developer action elements :

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

122 Content and presentation of evidence elements :

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

123 Evaluator action elements :

ADV_RCR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.1.3.7 AGD_ADM.1 Administrator guidance

124 Developer action elements :

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

125 Content and presentation of evidence elements :

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

126 Evaluator action elements :

AGD_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.1.3.8 AGD_USR.1 User guidance

127 Developer action elements :

AGD_USR.1.1D The developer shall provide user guidance.

128 Content and presentation of evidence elements :

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

129 Evaluator action elements :

AGD_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.1.3.9 ATE_COV.1 Evidence of coverage

130 Developer action elements :

ATE_COV.1.1D The developer shall provide evidence of the test coverage.

131 Content and presentation of evidence elements :

ATE_COV.1.1C The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

132 Evaluator action elements :

ATE_COV.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.1.3.10 ATE_FUN.1 Functional testing

133 Developer action elements :

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

134 Content and presentation of evidence elements :

ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

135 Evaluator action elements :

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.1.3.11 ATE_IND.2 Independent testing - sample

136 Developer action elements :

ATE_IND.2.1D The developer shall provide the TOE for testing.

137 Content and presentation of evidence elements :

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

138 Evaluator action elements :

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.1.3.12 AVA_SOF.1 Strength of TOE security function evaluation

139 Developer action elements :

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

140 Content and presentation of evidence elements :

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

141 Evaluator action elements :

AVA_SOF.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

5.1.3.13 AVA_VLA.1 Developer vulnerability analysis

142 Developer action elements :

AVA_VLA.1.1D The developer shall perform and document an analysis of the TOE deliverables searching for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2D The developer shall document the disposition of obvious vulnerabilities.

143 Content and presentation of evidence elements :

AVA_VLA.1.1C The documentation shall show, for all identified vulnerabilities, **including those identified in Appendix A of TFFPP v1.c.**, that the vulnerability cannot be exploited in the intended environment for the TOE.

144 Evaluator action elements :

AVA_VLA.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.1.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

5.1.4 Additional Security Assurance Requirements

145 This section includes the maintenance assurance requirements from the CC Part 3 that were not included in the TFFPP. They are restated verbatim from the CC.

5.1.4.1 ALC_FLR.1 Basic flaw remediation

146 Developer action elements:

ALC_FLR.1.1D The developer shall document the flaw remediation procedures.

147 Content and presentation of evidence elements:

ALC_FLR.1.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.1.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.1.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.1.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

148 Evaluator action elements:

ALC_FLR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.1.4.2 AMA_AMP.1 Assurance maintenance plan

149 Developer action elements:

AMA_AMP.1.1D The developer shall provide an AM Plan.

150 Content and presentation of evidence elements:

AMA_AMP.1.1C The AM Plan shall contain or reference a brief description of the TOE, including the security functionality it provides.

AMA_AMP.1.2C The AM Plan shall identify the certified version of the TOE, and shall reference the evaluation results.

AMA_AMP.1.3C The AM Plan shall reference the TOE component categorisation report for the certified version of the TOE.

AMA_AMP.1.4C The AM Plan shall define the scope of changes to the TOE that are covered by the plan.

AMA_AMP.1.5C The AM Plan shall describe the TOE life-cycle, and shall identify the current plans for any new releases of the TOE, together with a brief description of any planned changes that are likely to have a significant security impact.

AMA_AMP.1.6C The AM Plan shall describe the assurance maintenance cycle, stating and justifying the planned schedule of AM audits and the target date of the next re-evaluation of the TOE.

AMA_AMP.1.7C The AM Plan shall identify the individual(s) who will assume the role of developer security analyst for the TOE.

AMA_AMP.1.8C The AM Plan shall describe how the developer security analyst role will ensure that the procedures documented or referenced in the AM Plan are followed.

AMA_AMP.1.9C The AM Plan shall describe how the developer security analyst role will ensure that all developer actions involved in the analysis of the security impact of changes affecting the TOE are performed correctly.

AMA_AMP.1.10C The AM Plan shall justify why the identified developer security analyst(s) have sufficient familiarity with the security target, functional specification and (where appropriate) high-level design of the TOE, and with the evaluation results and all applicable assurance requirements for the certified version of the TOE.

AMA_AMP.1.11C The AM Plan shall describe or reference the procedures to be applied to maintain the assurance in the TOE, which as a minimum shall include the procedures for configuration management, maintenance of assurance evidence, performance of the analysis of the security impact of changes affecting the TOE, and flaw remediation.

151 Evaluator action elements:

AMA_AMP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AMA_AMP.1.2E The evaluator shall confirm that the proposed schedules for AM audits and re-evaluation of the TOE are acceptable and consistent with the proposed changes to the TOE.

5.1.4.3 AMA_CAT.1 TOE component categorization report

152 Developer action elements:

AMA_CAT.1.1D The developer shall provide a TOE component categorization report for the certified version of the TOE.

153 Content and presentation of evidence elements:

AMA_CAT.1.1C The TOE component categorization report shall categorise each component of the TOE, identifiable in each TSF representation from the most abstract to the least abstract, according to its

relevance to security; as a minimum, TOE components must be categorised as one of TSP-enforcing or non-TSP-enforcing.

AMA_CAT.1.2C The TOE component categorization report shall describe the categorization scheme used, so that it can be determined how to categorise new components introduced into the TOE, and also when to re-categorise existing TOE components following changes to the TOE or its security target.

AMA_CAT.1.3C The TOE component categorization report shall identify any tools used in the development environment that, if modified, will have an impact on the assurance that the TOE satisfies its security target.

154 Evaluator action elements:

AMA_CAT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AMA_CAT.1.2E The evaluator shall confirm that the categorization of TOE components and tools, and the categorization scheme used, are appropriate and consistent with the evaluation results for the certified version.

5.2 Security Requirements for the IT Environment

155 The TOE has no security requirements allocated to its IT environment.

6 TOE SUMMARY SPECIFICATION

- 156 This section presents a functional overview of the TOE; the security functions implemented by the TOE; and the Assurance Measures applied to ensure their correct implementation.
- 157 The following paragraphs briefly summarize which security functions implement specific the functional requirements specified in Section 5.1.1, TOE Security Functional Requirements:
- 158 Component **FAU_GEN.1**, audit data generation, is implemented by the Firewall Appliance (FA) and the System Management Server (SMS). The SMS makes a non-volatile record (audit) of all security audit events, management, or maintenance of the LMF. (LMF_AUDIT).
- 159 Component **FAU_SAR.1**, audit review, is accomplished via the SMS. The SMS provides the administrator reports wizards to filter and sort audit data. (LMF_AUDIT).
- 160 Component **FAU_SAR.3 (1) and (2)**, selectable audit review, is implemented via the SMS. The SMS report wizards allow for sorting and filtering of all attributes identified. The procedures for filtering and sorting the log files are provided in the ADM document. (LMF_AUDIT).
- 161 Component **FAU_STG.1**, protected audit trail storage, is implemented by the resident operating system. The log files are stored on the resident operating system and the assumed secure basic configuration requires physical and logical separation to permit access to only authorized administrators. The IGS document will provide procedures for setting file and directory permissions for protecting the audit files. (LMF_INA; LMF_AUDIT).
- 162 Component **FAU_STG.4**, prevention of audit data loss, is implemented by the SMS. If either the Sessions or Admin Events log grows to the maximum size allowed, then a new log is created and subsequent network data is recorded in the new log. Logs roll over at midnight, so there are never records from two different days in the same log file or when a configurable file size is reached (default = 10 MB for sessions, 1 MB for events). (LMF_AUDIT)
- 163 Component **FDP_IFC.1**, The UNAUTHENTICATED subset information flow control, is implemented by the FA. The FA controls the flow of incoming and outgoing IP packets. The default is **DROP**, which means the brick will discard the packet and not allow it through. Unless an authorized administrator explicitly configured the brick to accept requests based on specific security attributes, the LMF will successfully reject any and all requests. (LMF_UDP)

- 164 Component **FDP_IFF.1**, The UNAUTHENTICATED simple security attributes is implemented by the FA. Security attributes include security policy specified rules, host groups, service groups, dependency masks, and VPN information generated by the SMS on behalf of the Administrators. In addition, time-of-day, day-of-week, direction of access, physical Ethernet port, and existing session information can be used to determine whether or not a packet is allowed to pass in either direction. (LMF_UDP)
- 165 Component **FDP_RIP.1**, subset residual information protection, is implemented by the FA. The FA relies on internal pointers at the beginning and end of the packet to ensure subset residual information protection. (LMF_UDP)
- 166 Component **FIA_ATD.1**, user attribute definition associated with the authorized administrators is managed by the SMS. The SMS is responsible for maintaining administrator account information and providing administrator privilege information for enforcement. It provides the Administrator with the capability to create or update Administrator accounts. Account creation and management includes specifying privileges. The SMS is responsible for generating zone security policies on behalf of the Administrators and for managing the administrator's session while communicating with the SMS using a multi-threaded application. This means that SMS maintains the administrator's session status and keeps it separate from other ongoing administrator sessions. (LMF_INA).
- 167 Component **FIA_UAU.1**, timing of authentication for the administrators will be provided by the resident operating system.(LMF_INA)
- 168 Component **FIA_UID.2**, user identification before any action for the administrators is provided by the resident operating system. (LMF_INA).
- 169 Component **FMT_MOF.1**, management of security functions behavior has several security functions associated with this SFR. Both the resident operating system and SMS combine to provide this functionality. (LMF_SMAN)
- 170 Component **FMT_MSA.3** static attribute initialization functionality is provided by the TOE. Specific instructions are provided in the IGS documentation to ensure this requirement is met. (LMF_SMAN)
- 171 Component **FMT_SMR.1**, security roles, is provided by the SMS. (LMF_SMAN)
- 172 Component **FPT_RVM.1**, non-bypassability of the TSP of the TOE s provided by a combination of the basic configuration and enforcement of the security policy rules.(LMF_PSF)

- 173 Component **FPT_SEP.1**, TSF domain separation is implemented by the TOE. The FA, the SMS, and resident operating system combine to perform this security functionality. (LMF_PSF)
- 174 Component **FPT_STM.1**, Reliable time stamps is implemented by the resident operating system, the FA, and the SMS. The LMF preserves the sequence of events in the log files by timestamping. The FA preserves the order of the packet and sends the information to the SMS. The SMS respects the ordering of the FA and provides a timestamp using the clock setting on the resident operating system. (LMF_PSF)

6.1 TOE Security Functions

- 175 This section presents the security functions performed by the TOE.

6.1.1 Security Management [LMF_SMAN]

- 176 The SMS provides all LMF security management capabilities. By means of it, administrators manage the security policy rules enforced by associated FAs, audit mechanism configuration parameters, and administrator accounts. Only an authorized administrator working through the SMS on an NT or Solaris Server can perform security management functions to include creating and editing security policy, creating administrator accounts and modifying and setting thresholds for auditable events, and creating, modifying, deleting, and viewing rules regarding routing of information. The secure LMF configuration assumes only authorized administrators will have access to LMF environment containing the SMS and its resident operating system. Any administrative actions conducted by the resident operating system are restricted to authorized administrators. These actions are logged by the resident operating system and include:
- a) Modification of the time and date on the SMS. (FA does not have timestamp.)
 - b) Backup and recovery
- 177 Section 2.4 and 2.5 of the *LMF Systems Administrator Reference Manual*, Version 4.0 provides information on secure direct and remote accessing of the SMS. Logging into the SMS from the workstation on which it is running is the evaluated secure configuration. The SMS
- a) generates zone security policies on behalf of the Administrators. This responsibility includes taking the Administrator zone security policy specified rules, host groups, service groups, dependency masks, and VPN information and encoding it (policy compilation) into a file format suitable for local storage and/or downloading to a Brick Subsystem.
 - b) manages administrator accounts by maintaining the Certificate of Authority (CA) public key, performing system and administrator account management, and privilege preservation.

- c) maintains the Administrator account information. The SMS maintains for each System Administrator their UserID, password, domain, role, and privileges.
- d) preserves the System Administrator's privilege information and provides it for enforcement.
- e) enforces System Administrator privileges. Privilege enforcement is based upon a privilege vector that is returned to it in response to a System Administrator login attempt. The privilege vector identifies the role (administrator or zone administrator) and identifies the System Administrators access permissions representing r/w/x for {access, audit, accounts, system}.
- f) logs the System Administrator out if unrecognized data is received from the System Administrator interface or un-handled exceptions occur within SMS Subsystems.
- g) receives System Administrator edits to policy information and writes the information to policy files within the domain directory.
- h) receives System Administrator edits to account information and passes the information for incorporation into files within the admin directory for system retention.
- i) receives System Administrator edits to alarm configuration information and writes the information to action, trigger, alarmConfig files within the load directory for system retention.
- j) receives System Administrator edits to zone information and writes the information to zone files within the file system for system retention.
- k) receives System Administrator edits to firewall information and writes the information to the firewalls directory.

- 178 The Firewall Appliance (FA) permits the security policies to be loaded into the FA from the SMS over an authenticated and encrypted session. Each security policy's digital signature is verified before the policy is loaded (the policies are digitally signed by the SMS using the firewall administrator's certificate when created or edited). The administration applications also provide system status information.
- 179 Loading a FA loads the Zone Assignment Table on the FA. The Zone Assignment Table identifies the zones that are assigned to each of the FA's interfaces.
- 180 The Media Access Control table contains the IP addresses of all local machines. The session cache identifies all active sessions traversing a FA. The FA applies the zone security policy to the first session packet it detects and not to subsequent packets within the same session.
- 181 **Functional Requirements Satisfied:** FMT_MOF.1, FMT_MSA.3, and FMT_SMR.1

6.1.2 Identification and Authentication [LMF_INA]

182 There are two aspects of this security function that require strength of
function rating. The authentication mechanisms used to authenticate the
administrator and the single-use authentication mechanism have a
probabilistic nature. Their SOF claim is SOF-basic. In addition, they must
satisfy the following requirements:

183 The probability of authentication data being guessed will be less than one
in a million, and

184 At least one System Administrator is required to administer an installation
of the SMS. A System Administrator is defined as a person who logs into
the SMS as a System Administrator and has System Administrator
privileges. The first System Administrator login is created automatically
during the software installation process. This administrator can then
create other administrator accounts. The assumed secure basic
configuration is physically and logically isolated and only authorized
administrators will have physical access to the SMS server. The SMS
software will be the only software on the server in addition to the benign
resident operating system software. The FA has no user (including
administrator) accounts. The SMS requires administrators to identify and
authenticate themselves before they can perform any other SMS actions.

Table 15. Administrator Account Information

Field	Description
AdminID	The administrator's login.
Full Name	The administrator's name.
Role	System or Zone Administrator
Zone	The zones this administrator will be permitted to access.
Password	The password required to validate the login.
Verify Password	The password, entered exactly as above.
Phone Number	The administrator's office telephone number.
Email Number	The administrator's email address.
Pager Info	The PIN of the administrator's paging service.
Expiration Date	The date the account expires.

185 The System Administrator establishes communication with the SMS by
launching the Netscape Communicator 4.05 browser and specifying the
Universal Resource Locator (URL) for the SMS's Login Screen. The
browser then establishes a HyperText Transport Protocol (HTTP) Secure
Session Layer (SSL) connection with the SMS and displays the SMS
Login Screen to the System Administrator. The Client/GUI Subsystem is
now communicating with the *Netscape Enterprise Server* (NES)
Subsystem.

- 186 Secure session establishment is displayed to the System Administrator by displaying the security indicator at the bottom-left of the Navigator window as a closed padlock. If the browser fails to establish a secure session, the security indicator will remain an open padlock.
- 187 The System Administrator provides his userID and password within the browser window. A login servlet is launched by the NES Subsystem when the System Administrator provides his userID and password. The servlet passes this information to the (Remote Administration Daemon) RAD Subsystem through a file interface and abides by its access control decision. After identifying and authenticating the System Administrator, an applet is downloaded to the System Administrator's desktop to provide the Primary User Interface and to secure the communications between the applet and the Remote Administration Process (RAP) Subsystem.
- 188 The SMS manages the System Administrator's interface. This includes interacting with the System Administrator management screens presented within the GUI JVE to provide the appropriate Java™ Applet in response to System Administrator's input. Such interactions include – based on System Administrator input, presenting the System Administrator interface the appropriate applet for management of System Administrator accounts, alarms, logging, and zone management.
- 189 These capabilities enable an administrator to access the SMS on the system console.
- 190 The SMS uses the System Administrator account information to make authentication decisions based upon the userID and password provided to it by the NES Subsystem (servlet) via its file interface with the servlet.
- 191 **Functional Requirements Satisfied:** FIA_ATD.1, FIA_UAU.1, and FIA_UID.2.

6.1.3 User Data Protection [LMF_UDP]

- 192 The FA controls the flow of incoming and outgoing IP packets. The default is **DROP**, which means the brick will discard the packet and not allow it through. Unless an authorized administrator explicitly configured the brick to accept requests based on specific security attributes, the LMF will successfully reject any and all requests.
- 193 The FA works with data at the IP packet level. Security rules in the security policy perform this filtering function by looking at five basic pieces of information (security attributes) in each packet to see if they match the same information in the rule.
- a) The direction of the packet.

- b) The source host (the presumed address)
 - Single host if source is a single machine, this field will contain its IP address.
 - Host group if the source is a group of machines, this field will contain the host group name. (A host group is a collection of IP addresses. It can consist of one or more single addresses, or ranges of addresses. Host groups are created by the system administrator prior to creating the rule.)
- c) The destination host (the presumed address)
 - Single host if destination is a single machine, this field will contain its IP address.
 - Host group if the destination is a group of machines, this field will contain the host group name. A host group is a collection of IP addresses. It can consist of one or more single addresses, or ranges of addresses. Host groups are created by the system administrator prior to creating the rule.)
- d) The service or protocol: Every security rule must specify an Internet service. Services are application-level protocols that are identified by their destination TCP or UDP port numbers. There are three ways to enter this information.
 - Protocol name or number
 - Protocol number/destination port
 - Protocol number/destination port/source port
 - For ICMP messages, the format is protocol/type/code.
- e) The action taken by the rule. This field defines the action that the brick will take when it encounters a packet that matches all the information in the above four fields. The default is **DROP**, which means the brick will discard the packet and not allow it through. To allow a packet matching the above four fields through the brick, the field must be set to **PASS**.

The FA extracts information from the IP packet header and applies rules from a security policy. Information within an IP packet that is used to make access control decisions includes source and destination TCP or UDP port number, and packet type.

- 195 Security attributes include security policy specified rules, host groups, service groups, dependency masks, and VPN information generated by the SMS on behalf of the Administrators. In addition, time-of-day, day-of-week, direction of access, physical Ethernet port, and existing session information can be used to determine whether or not a packet is allowed to pass in either direction.
- 196 The SMS provides a network address translation feature that permits three types of address translation:
- 197 Source Address Mapping
- 198 Destination Address Mapping
- 199 Destination Port Mapping.
- 200 Address translation is activated by a basic security rule. When a packet matching the rule arrives at the brick, the source or destination address, or destination port, in the packet's header is changed, or mapped, to the address or port provided by the SMS.
- 201 The FA relies on internal pointers at the beginning and end of the packet to ensure full residual information protection.
- 202 **Functional Requirements Satisfied:** FDP_IFC.1, FDP_IFF.1, and FDP_RIP.1

6.1.4 Protection of Security Functions [LMF_PSF]

- 203 Non-bypassability of the TOE is provided by a combination of the basic configuration and enforcement of the security policy rules. The assumed secure basic configuration maintaining physical and logical isolation supports the Protection of Security Functions (PSF). To further ensure that security functions on the FA cannot be tampered with or bypassed, the security functions are embedded in the Inferno™ operating system kernel. The FA has no user (including administrator) accounts. This implementation provides the required TSF domain separation. SMS security functions, implemented as Inferno daemons and Java™ applets, are protected by Hosted Inferno and by the Netscape Java™ Virtual Machine (JVM). The security policy rules enforced by the FA are applied to every packet.
- 204 The FA is equipped with four auto-sensing 10/100Base-T Ethernet interface cards and can be positioned between any type of Ethernet-based network elements (e.g., routers, hubs, switches, servers, PCs).
- 205 The FA does not contain a hard drive and can be deployed without a monitor and keyboard. Other than a floppy disk drive for initial software

boot, it has a minimum of moving parts those being an on/off switch and a power supply fan.

206 Tools used to backup and restore the configuration files are the tools provided by the native operating system (NT or Solaris). The configuration files are distributed across the file system that belongs to the server's native operating system. The secure LMF configuration assumes only authorized administrators will have access to LMF environment containing the SMS and its resident operating system.

207 The subject separation is provided by the SMS. The SMS enforces System Administrator privileges. Privilege enforcement is based upon a privilege vector that is returned to it in response to a System Administrator login attempt. The privilege vector identifies the role (administrator or zone administrator) and identifies the System Administrators access permissions representing r/w/x for {access, audit, accounts, system}.. SMS logs the System Administrator out if unrecognized data is received from the System Administrator interface or un-handled exceptions occur within SMS Subsystems.

208 Functional Requirements Satisfied: FPT_RVM.1, FPT_SEP.1

6.1.5 Audit [LMF_AUDIT]

209 The FA detects the occurrence of selected events, gathers information concerning them, and sends that information to the SMS, where it is stored. The SMS also detects the occurrence of selected events (e.g., security administrator actions), gathers information concerning them, and records it. Audit reporting and alarm features are also provided by the SMS. The reporting feature of the LMF allows Administrators to view and analyze internal and system information of the LMF. Using Report Wizards, audit event items can be extracted and presented in a legible and coherent format.

210 The types of audit events recorded in AdminEvents Log and the Sessions Log are contained in a Appendix B of *LMF System Administrators Manual*, Version 4.0 and they include but are not limited to the following:

- a) Modifications to group of authorized administrator
- b) Use of user identification mechanism
- c) Any use of the authentication mechanism
- d) Reaching the unsuccessful authentication attempt threshold .

211 The audit log will record at a minimum the following information:

- a) Type of message(audit event)

- b) Source type (b for messages originating from the brick; I for messages originating from the SMS.
- c) Source (firewall name or a SMS subsystem)
- d) Timestamp
- e) Subtype

212 Additional audit log fields can be defined to include source IP and results. The information contained the audit logs can retrieved through filtering and sorting options provided in the Reporting subsystem. Reports are based on records of an audit log. Each line in an audit log is a record. A record consists of fields and each field contains a value. Some fields can be filtered to look for specific user-defined values. Logical “AND” and “OR” functions can be performed across filterable fields. A report ‘wizard’ permits specifying value for filterable fields to hone in on field criteria values. The ‘wizard’ permits selection of fields on which to sort and indicated sorting direction (ascending or descending). When generating an Admin Events or Sessions Log report, the ability to search the raw log file by entering a text string is also provided.

6.1.5.1 Audit Generation

213 The FA records the start and end of a session. It extracts information from the session cache to uniquely identify each session, and it records:

- a) Start and stop times
- b) Action taken
- c) Statistics, such as number of bytes and packets passed

214 The FA bundles this information into an audit message and sends it to an awaiting audit server, located on the SMS.

215 The SMS logs session info sent to it by FA, and logs operational information from all SMS Subsystems (including FA Subsystems). The SMS reformats the log events it receives, applies a time stamp, and writes the event to the appropriate log file. The SMS uses the NT or Solaris clock on the motherboard to generate timestamps for audit records.

216 Functional Requirements Satisfied: FAU_GEN.1, FPT_STM.1

6.1.5.2 Audit Review

217 The SMS makes a non-volatile record (audit) of all security audit events, management, or maintenance of the LMF, and it enables an Administrator to view critical user and system information, e.g., FA up/down status and logged on users, etc. It also enables Administrators to monitor the

configuration of and access to the FAs deployed throughout the network. Reports are generated using logged administrative events and FA session log data. The SMS provides the Administrator with an automated tool that reviews audit logs for configurable alarming events, and when found, to notify the System Administrator.

218 Functional Requirements Satisfied: FAU_SAR.1 and FAU_SAR.3 (1) and (2))

6.1.5.3 Audit Storage

219 The log files are separated into two different directories: sessions and admin events.

- a) One for “sessions” data, containing information about traffic through the brick.
- b) One for “admin events”: logins and actions of administrators, errors, contacting and losing bricks, and pretty much everything else except information about brick traffic.
- c) In each directory, the filenames are assigned in the same way. The purpose of the assignment algorithm is to assure that a lexical sort by filename also provides a chronological sort of the data in the files. This improves performance in reading log files for reports and alarms.

220 The SMS provides the authorized administrator with the capability to configure the log file maximum size and the amount of disk space to allocate for all logs. When the contents of the log directory reaches the configured size, the SMS also provides the authorized administrator with the ability to configure for each FA to reclaim disk space by deleting the oldest log file for that FA or to not lose audit data. This last feature ensures that network traffic will be stopped on a FA-by-FA basis until space has been made available on the SMS for additional audit data.

221 The default audit trail size is 1 Gbyte and can be configured by the user. The Logging Subsystem has been hard coded to provide 90% of the audit trail allocation to the session log files and 10% of its allocation to the admin log files. The maximum audit file size is 10 Mbytes. When an audit file reaches 10 Mbytes or a new day is started, the Logging Subsystem closes the current log file and starts a new audit file. There is always one open session and admin log file open to record session and admin log events.

222 If the SMS has been configured to reclaim disk space for all managed FA, then audit storage can never be exhausted. If the session log files reach the configured maximum allocation (and the SMS for that FA has been configured to reclaim disk space) then, the oldest session log file will be removed to create space for a new session log file. If the admin log files reach the configured maximum allocation (and the SMS has been

configured to reclaim disk space), the oldest admin log file will be removed to create space for a new admin log file. This audit architecture ensures that storage for audit data will never be exhausted and cause the FA to stop passing traffic or the SMS from performing properly.

223 If the SMS has been configured to stop traffic rather than delete a log file, then all customer traffic through bricks will halt. It will stop when the brick's own audit buffer is full, and remain blocked until there is space allocated for log data once again. This capability can be separately configured for each of the logs (admin, sessions, eua, and promon). To assist in managing this capability:

224 Version 4.0 has proactive monitoring alarms to warn that log allocations are filling up.

225 Version 4.0 has an error alarm that can tell you that the logs have filled and traffic has been halted.

226 The SMS enables Administrators to monitor the configuration and traffic mediation of the firewalls deployed throughout the network. The report “wizards” are displayed to enable Administrators to filter and sort data. Through this interface, the System Administrator has the capability to generate “Memorized Reports” (i.e., report templates) and to generate Closed Session, Session; and Administrative Events reports.

227 The SMS enables an Administrator to view critical System Administrator and system information to view:

- a) the identities of all logged in system users,
- b) their session duration,
- c) IP address of the host they logged in from, and
- d) The status of the communication link between each brick and the SMS.

228 The SMS provides the LMF System with a real-time alarming capability. In a manner similar to the creation of management reports, alarms can be specified using a wizard to define an alarm. The alarms feature of the LMF allows Administrators to configure alarmable events and the action(s) taken when and if these events occur in the system.

229 Functional Requirements Satisfied: FAU_STG.1 and FAU_STG.4

6.2 Assurance Measures

230 The TOE satisfies the SARs specified in the TFFPP. This section identifies the Configuration Management, System Delivery Procedures, System Development Procedures, Guidance Documents, Testing, and

Vulnerability Analysis measures applied by Lucent to satisfy the CC EAL2 assurance requirements.

6.2.1 Configuration Management

231 The Configuration Management measures applied by Lucent include assigning a unique product identifier for each release of the TOE. Associated with this Product Identifier is a list of Hardware and Software configuration items that comprise a single instance of the TOE. These configuration management measures are documented within the following Lucent Document: Lucent Managed Firewall Version 4.0, Configuration Management, Version 2.0.

232 Assurance Requirements Satisfied: ACM_CAP.2

6.2.2 Delivery and Operation

233 Lucent provides Delivery and Operation documentation that describes what components are delivered with the LMF, guidance for initially installing it, and warnings about the importance of properly unpacking, installing and configuring the TOE. These deliver and operation measures are documented within the following Lucent documents:

- a) Lucent Managed Firewall Version 4.0, Delivery, Installation, Generation, and Start-Up Procedures (Version 8.3)
- b) Lucent Managed Firewall Security Management Server Version 4.0(i) Installation Guide.

234 Assurance Requirements Satisfied: ADO_IGS.1 and ADO_DEL.1

6.2.3 Development

235 The Lucent architecture documents satisfy the functional specification and high-level design information requirements, and provide a correspondence between that information and this ST. These architecture measures are documented within the following Lucent documents:

- a) Lucent Managed Firewall Version 4.0, Functional Specification (Version 2.2)
- b) Lucent Managed Firewall Version 4.0, High Level Design (Version 2.2)
- c) Lucent Managed Firewall Version 4.0, Correspondence Document (Version 2.1)

236 **Assurance Requirements Satisfied:** ADV_FSP.1, ADV_HLD.1, and ADV_RCR.1

6.2.4 Guidance

237 The Guidance Documents provided by Lucent include both the Installation and Configuration manuals that guide administrators through the process of unpacking, installing, and configuring the LMF. These guidance measures are documented within the following Lucent documents:

- a) Lucent Managed Firewall Version 4.0, Delivery, Installation, Generation, and Start-Up Procedures, Version 8.3.
- b) Lucent Managed Firewall Version 4.0 Administration Guidance, Version 1.0, Draft, August 30, 1999.
- c) Lucent Managed Firewall Security Management Server Version 4.0(i) Installation Guide.
- d) Lucent Managed Firewall Security Management Server Version 4.0(i) System Administrator Reference Manual
- e) Lucent Managed Firewall Security Management Server Version 4.0(i) Zone Administrator Reference Manual

238 Assurance Requirements Satisfied: AGD_USR.1 and AGD_ADM.1

6.2.5 Vulnerability Analysis

239 As part of the design and testing process, Lucent conducted Vulnerability Analysis of the LMF. The goal of the analysis was to identify any obvious weaknesses that could be exploited by an attack. In addition to the testing conducted by CSC, ISS Real Secure also conducted preliminary vulnerability analysis. The vulnerability analysis is document within the following Lucent document:

- a) Lucent Managed Firewall Vulnerability Assessment, version 4.0, Vulnerability Analysis, version 2.1.

240 Assurance Requirements Satisfied: AVA_VLA.1

6.2.6 Test

241 Lucent performs extensive Testing of the LMF. The testing performed includes both functional and penetration testing to ensure that the LMF meets its design goals. These tests are documented in the following Lucent documents:

- a) Lucent Managed Firewall version 4.0 Functional Testing Version 2.2.
- b) Lucent Managed Firewall R4.0 Proactive Monitoring Feature Test Plan, February 15, 1999

- c) LMF v4.0 User Model & Authentication Testing, March 3, 1998
- d) Lucent Managed Firewall, Release 4.0, Lucent Proxy Agent- Virus Scanning Test Plan, June 11, 1999
- e) Lucent Managed Firewall Release 4.0 Content Security - URL Blocking/Filtering Testing, March 1, 1999
- f) Lucent Managed Firewall R4.0 SMS Failover Test Plan
- g) Lucent Managed Firewall R4.0 Regression Test Plan

242 **Assurance Requirements Satisfied:** ATE_FUN.1, ATE_COV.1, and ATE_INT.2

6.2.7 Strength of Function Analysis

243 The Strength of Function Analysis performed on Timing of Authentication is provided within the following Lucent document:

- a) Lucent Managed Firewall Version 4.0 Administrator Guidance, Version 1.0.

244 Assurance Requirements Satisfied: AVA_SOF.1

6.2.8 Maintenance of Assurance

245 Lucent's plans and procedures to ensure the LMF version 4.0 continues to meet its security target after certification are provided with the following Lucent documents:

- a) Lucent Managed Firewall Version 4.0 Assurance Maintenance (AM) Plan, Version 1.0.
- b) Lucent Managed Firewall Version 4.0 Categorization Report, Version 1.0.

246 Assurance Requirements Satisfied: AMA_AMP.1, AMA_CAT.1, and ALC_FLR.1

7 PP CLAIMS

247 This section provides the PP conformance claim statements.

7.1 PP Reference

248 The TOE conforms to the U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments, Version 1.1, April 1999.

7.2 PP Refinements

249 The following PP requirements were further refined for this Security Target:

- a) FAU_GEN.1 Audit data generation
- b) FDP_IFF.1 Simple security attributes
- c) FIA_ATD.1 User attribute definition
- d) FAU_SAR.3 (1) Selectable Audit Review
- e) FAU_SAR.3 (2) Selectable Audit Review
- f) FAU_STG.1 Protected audit trail storage
- g) FMT_MSA.3 Static attribute initialization
- h) FMT_MOF.1 Management of security functions behavior
- i) AVA_VLA.1 Developer vulnerability analysis

250 In the case of FAU_SAR.3, the refinement interprets the TFFPP SFR to require that LMF be capable of searching the audit data for user identity, presumed subject address, ranges of dates, ranges of time, and ranges of IP address and sorting audit data based on chronological order of occurrence. LMF satisfies this SFR interpretation.

251 In the case of AVA_VLA.1, the refinement specifies the minimum identified vulnerabilities for which the evaluated LMF must be analyzed.

7.3 PP Additions

252 The assurance maintenance SARs were added to utilize the certification of the previous LMF version.

7.4 Rationale for not implementing all PP security objectives

253 The ST does not include the following TOE and environment security objectives: O.ENCRYPT, O.LIMEXT, and OREMACC. These security objectives are relevant to secure remote administration of the TOE. These objectives are beyond the scope of this evaluation.

8 RATIONALE

8.1 Rationale For IT Security Objectives

- O.IDAUTH This security objective is necessary to counter the threat: T.NOAUTH because it requires that users be uniquely identified before accessing the TOE.
- O.MEDIAT This security objective is necessary to counter the threats: T.ASPOOF, T.MEDIAT and T.OLDINF, which have to do with getting impermissible information to flow through the TOE. This security objective requires that all information that passes through the networks is mediated by the TOE and that no residual information is transmitted.
- O.SECSTA This security objective ensures that no information is comprised by the TOE upon start-up or recovery and thus counters the threats: T.NOAUTH and T.SELPRO.
- O.SELPRO This security objective is necessary to counter the threats: T.SELPRO and T.AUDFUL because it requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with TOE security functions.
- O.AUDREC This security objective is necessary to counter the threat: T.AUDACC by requiring a readable audit trail and a means to search and sort the information contained in the audit trail.
- O.ACCOUN This security objective is necessary to counter the threat: T.AUDACC because it requires that users are accountable for information flows through the TOE and that authorized administrators are accountable for the use of security functions related to audit.
- O.SECFUN This security objective is necessary to counter the threats: T.NOAUTH, and T.AUDFUL by requiring that the TOE provide functionality that ensures that only the authorized administrator has access to the TOE security functions.

Table 16: Mapping Of Threats To Security Objectives

	T.NOAUTH	T.ASPOOF	T.MEDIAT	T.OLDINF	T.AUDACC	T.SELPRO	T.AUDFUL
O.IDAUTH	X						
O.MEDIAT		X	X	X			
O.SECSTA	X					X	
O.SELPRO						X	X
O.AUDREC					X		
O.ACCOUN					X		
O.SECFUN	X						X

8.2 Rationale For Security Objectives For The Environment

O.LOWEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.

O.PUBLIC The TOE does not host public data.

O.NOEVIL Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.

O.SINGEN Information can not flow among the internal and external networks unless it passes through the TOE.

O.SECFUN With the exception of identification and authentication, there are no security functions on the TOE accessible to human users who are not authorized administrators.

O.NOREMO With the exception of identification and authentication, human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.

O.PHYSEC The processing resources of the TOE that depend on hardware security features will be located within controlled access facilities that mitigate unauthorized, physical access.

O.GENPUR The TOE only stores and executes security-relevant applications and only stores data required for its secure operation.

O.DIRECT The TOE is available to authorized administrators only.

O.GUIDAN This non-IT security objective is necessary to counter the threat: T.TUSAGE because it requires that those responsible for the TOE ensure that it is delivered, installed, administered, and operated in a secure manner.

O.ADMTRA This non-IT security objective is necessary to counter the threat: T.TUSAGE because it ensures that authorized administrators receive the proper training. O.ADMTRA also counters the threat T.AUDACC by helping ensure the audit logs are reviewed.

Table 17: Mappings Between Threats/Assumptions and Security Objectives for the Environment

	T.TUSAGE	T.AUDACC	A.LOWEXP	A.PUBLIC	A.NOEVIL	A.SINGEN	A.SECFUN	A.NOREMO	A.PHYSEC	A.GENPUR	A.DIRECT
O.GUIDAN	X										
O.ADMTRA	X	X									
O.LOWEXP			X								
O.PUBLIC				X							
O.NOEVIL					X						
O.SINGEN						X					
O.SECFUN							X				
O.NOREMO								X			
O.PHYSEC									X		
O.GENPUR										X	
O.DIRECT											X

8.3 Rationale For Security Requirements

- 254 The rationale for the chosen level of SOF-basic is based on the low attack potential of the threat agents identified in this security target. Those security objectives imply probabilistic or permutational security mechanism and that the metrics defined are the minimal “industry” accepted (for the passwords) and government required (for the encryption) metrics they should be good enough for SOF-Basic.

FMT_SMR.1 Security roles

- 255 Each of the CC class FMT components in this Security Target depend on this component. It requires the ST writer to choose a role(s). This component traces back to and aids in meeting the following objective: O.SECFUN.

FIA_ATD.1 User attribute definition

- 256 This component exists to provide users with attributes to distinguish one user from another, for accountability purposes and to associate the role chosen in FMT_SMR.1 with a user. This component traces back to and aids in meeting the following objectives: O.IDAUTH.

FIA_UID.2 User identification before any action

- 257 This component ensures that before anything occurs on behalf of a user, the users identity is identified to the TOE. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.ACCOUN.

FIA_UAU.1 Timing of authentication

- 258 This component ensures that users are authenticated at the TOE. The TOE is permitted to pass information before users are authenticated. Authentication must occur whether the user is a human user or not and whether or not the user is an authorized administrator. If the authorized administrator was not always required to authenticate, there would be no means by which to audit any of their actions. An additional SOF metric for this requirement is defined in section 5.1.1.1 to ensure that the authentication mechanism chosen cannot be easily bypassed. This component traces back to and aids in meeting the following objectives: O.IDAUTH.

FDP_IFC.1 Subset information flow control

259 This component identifies the entities involved in the UNAUTHENTICATED information flow control SFP (i.e., users sending information to other users and vice versa). This component traces back to and aids in meeting the following objective: O.MEDIAT.

FDP_IFF.1 Simple security attributes

260 This component identifies the attributes of the users sending and receiving the information in the UNAUTHENTICATED SFP, as well as the attributes for the information itself. Then the policy is defined by saying under what conditions information is permitted to flow. This component traces back to and aids in meeting the following objective: O.MEDIAT.

FMT_MSA.3 Static attribute initialization

261 This component ensures that there is a default deny policy for the information flow control security rules. This component traces back to and aids in meeting the following objectives: O.MEDIAT , O.SECSTA, and O.SECFUN.

FDP_RIP.1 Subset residual information protection

262 This component ensures that neither information that had flowed through the TOE nor any TOE internal data are used when padding is used by the TOE for information flows. This component traces back to and aids in meeting the following objective: O.MEDIAT.

FPT_RVM.1 Non-bypassability of the TSP

263 This component ensures that the TSF are always invoked. This component traces back to and aids in meeting the following objective: O.SELPRO.

FPT_SEP.1 TSF domain separation

264 This component ensures that the TSF have a domain of execution that is separate and that cannot be violated by unauthorized users. This component traces back to and aids in meeting the following objective: O.SELPRO.

FPT_STM.1 Reliable time stamps

265 FAU_GEN.1 depends on this component. It ensures that the date and time on the TOE is dependable. This is important for the audit trail. This component traces back to and aids in meeting the following objective: O.AUDREC.

FAU_GEN.1 Audit data generation

266 This component outlines what data must be included in audit records and what events must be audited. This component traces back to and aids in meeting the following objectives: O.AUDREC and O.ACCOUN.

FAU_SAR.1 Audit review

267 This component ensures that the audit trail is understandable. This component traces back to and aids in meeting the following objective: O.AUDREC.

FAU_SAR.3 Selectable audit review

268 This component ensures that a variety of searches and sorts can be performed on the audit trail. This component traces back to and aids in meeting the following objective: O.AUDREC.

FAU_STG.1 Protected audit trail storage

269 This component is chosen to ensure that the audit trail is protected from tampering. Only the authorized administrator is permitted to do anything to the audit trail. This component traces back to and aids in meeting the following objectives: O.SELPRO and O.SECFUN.

FAU_STG.4 Prevention of audit data loss

270 This component ensures that the authorized administrator will be able to take care of the audit trail if it should become full. But this component also ensures that no other auditable events as defined in FAU_GEN.1 occur. Thus the authorized administrator is permitted to perform potentially auditable actions though these events will not be recorded until the audit trail is restored to a non-full status. This component traces back

to and aids in meeting the following objectives: O.SELPRO and O.SECFUN.

FMT_MOF.1 Management of security functions behavior

271 This component was chosen and modified to some extent via permitted CC operations in an attempt to consolidate all TOE management/administration/security functions. This component traces back to and aids in meeting the following objectives: O.SECFUN, and O.SECSTA

Table 18: Mappings Between TOE Security Functions and IT Security Objectives

	O.IDAUTH	O.MEDIAT	O.SECSTA	O.SELPRO	O.AUDREC	O.ACCOUN	O.SECFUN
FMT_SMR.1							X
FIA_ATD.1	X						
FIA_UID.2	X					X	
FIA_UAU.1	X						
FDP_IFC.1(1)		X					
FDP_IFF.1(1)		X					
FDP_IFC.1(2)		X					
FDP_IFF.1(2)		X					
FMT_MSA.3		X	X				X
FDP_RIP.1		X					
FPT_RVM.1				X			
FPT_SEP.1				X			
FPT_STM.1					X		
FAU_GEN.1					X	X	
FAU_SAR.1					X		
FAU_SAR.3 (1)					X		
FAU_SAR.3 (2)							
FAU_STG.1				X			X
FAU_STG.4				X			X
FMT_MOF.1			X				X

8.4 Rationale For Assurance Requirements

272

EAL2 was chosen to provide a low to moderate level of independently assured security in the absence of ready availability of the complete development record from the vendor. As such, minimal additional tasks are imposed upon the vendor to the extent that if the vendor applies reasonable standards of care to the development, evaluation may be feasible without vendor involvement other than support for functional testing and vulnerability testing verification. The chosen assurance level is consistent with the postulated threat environment. Specifically, that the threat of malicious attacks is not greater than moderate, and the product will have undergone a search for obvious flaws.

8.5 Rationale For Not Satisfying All Dependencies

273 Functional component FMT_MSA.3 depends on functional component FMT_MSA.1 Management of security attributes. In an effort to place all the management requirements in a central place, FMT_MOF.1 was used. Therefore FMT_MOF.1 more than adequately satisfies the concerns of leaving FMT_MSA.1 out of this Protection Profile.

8.6 Consistency and Mutually Supportive Rationale

274 The set of security requirements provided in this LMF ST form a mutually supportive and internally consistent whole as evidenced by the following:

- a) The choice of security requirements is justified as shown in Sections 8.3 and 8.4. The choice of SFR and SARs were made based on the assumptions about, the objectives for, and the threats to the TOE and the security environment. This ST provides evidence the security objectives counter threats to the TOE (Table 16), and also, the assumptions and objectives counter threats to the TOE environment (Table 17).
- b) The security functions of LMF satisfy the SFRs as shown in Table 18. All SFR dependencies have been satisfied with the exception of those noted in Section 8.5.
- c) The SOF claims are valid and are satisfied as shown in Section 8.3. The rationale for the chosen level of SOF-basic is based on the low attack potential of the threat agents identified in this security target. The identified metrics and SOF claim is commensurate with the EAL2 level of assurance.
- d) The SARs are appropriate for the assurance level of EAL2 and are satisfied by LMF version 4 and are satisfied as shown in Section 6.2. EAL2 was chosen to provide a low to moderate level of independently assured security in the absence of ready availability of the complete development record from the vendor.